

~~TOP SECRET//SI//NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

**EXHIBIT B**

**MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

2016 SEP 26 PM 12:26  
FEDERAL BUREAU OF INVESTIGATION  
U.S. DEPARTMENT OF JUSTICE

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court (FISC) of such activity.

(U) Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Similarly, nothing in these procedures shall prohibit the retention, processing, analysis, or dissemination of information necessary to comply with a specific congressional mandate or order of a court within the United States. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

~~TOP SECRET//SI//NOFORN~~

Classified by: ~~The Attorney General~~  
Derived From: ~~NSA/CSSM 1-52 (dated 20130930)~~  
Declassify On: ~~20410919~~

~~TOP SECRET//SI//NOFORN~~

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

- (a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.
- (b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.
- (c) (U) Communications of a United States person include all communications to which a United States person is a party.
- (d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.
- (e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.
- (f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.
- (g) (~~TS//SI//NF~~) Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [REDACTED] or multiple discrete communications [REDACTED].
- (h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

- (i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.
- (j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.
- (k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:
  - (1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.
  - (2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.
  - (3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.
  - (4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

## (b) (U) Monitoring, Recording, and Handling

- (1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.
- (2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.
- (3) (U) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.
- (4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques
  - a. (U) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.
    1. (U) Notwithstanding subsection 3(b)(4)a above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.
    2. (U) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

- (a) (U) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection 3(b)(4)a and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.
  - (b) (U) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b below and the other applicable provisions of these procedures.
  - (c) (U) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.
3. (U) Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a will be handled in accordance with subsection 3(b)(4)b below and the other applicable provisions of these procedures.
- b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.
    - 1. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.
    - 2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

- (a) (U) If the discrete communication is to, from, or about a tasked selector, any United States person information in that communication will be handled in accordance with the applicable provisions of these procedures.
  - (b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable United States person or a person reasonably believed to be located in the United States, that communication (including any United States person information therein) will be handled in accordance with the applicable provisions of these procedures.
  - (c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable United States person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the FISC of such use.
3. (U) An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1 and 2 above.
4. (U) Notwithstanding subsection 3(b)(4)b above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable United States person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures, which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information, as defined in FISA. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8, as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) (U) Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition.

Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) (U) Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

- (3) (U) Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.
- (4) (U) In addition, NSA will follow the following procedures:
- a. (U) Notwithstanding the destruction requirements set forth in these minimization procedures, NSA may retain specific section 702-acquired information if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The Department of Justice will identify in writing the specific information to be retained (including, but not limited to, the target(s) or selector(s) whose information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained. In order to restrict access to information being retained pursuant to this provision, personnel not working on the particular litigation matter shall not access the section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures.
1. (U) Each year, NSA will provide the Department of Justice's National Security Division with a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired data that would otherwise be subject to age off pursuant to these procedures, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible based on the information available to NSA, a description of the status of each such litigation matter.
  2. (U) In certain circumstances, NSA may receive written notice from the Department of Justice advising NSA to preserve section 702-acquired information that would otherwise be subject to a destruction requirement under Sections 3(b)(1), 3(b)(4), 3(c)(3), 3(d)(2), 3(e), 4, or 5. NSA will promptly provide the Department of Justice's National Security Division with a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired information that would otherwise be subject to destruction pursuant to Sections 3(b)(1), 3(b)(4),

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

3(c)(3), 3(d)(2), 3(e), 4, or 5, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible based on the information available to NSA, a description of the status of each such litigation matter. When such circumstances arise, the Department of Justice's National Security Division will promptly notify the FISC.

- b. (U) The Department of Justice may advise NSA to retain specific section 702-acquired information subject to a destruction requirement other than those specified above in this section because such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. NSA will provide the Department of Justice's National Security Division with a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired information that would otherwise be subject to destruction, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible, based on the information available to NSA, a description of the status of each such litigation matter. The Department of Justice's National Security Division will promptly notify and subsequently seek authorization from the FISC to retain the material as appropriate and consistent with law. NSA will restrict access to and retain such information in the manner described in subparagraph 4(a), at the direction of the Department of Justice until either the FISC denies a government request for authorization to retain the information or the Department of Justice notifies NSA in writing that the information is no longer required to be preserved for such litigation matters. After receiving such notice, NSA shall promptly destroy the section 702-acquired information.

(d) (U) Change in Target's Location or Status

- (1) (U) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.
- (2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

- (e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [REDACTED] post-tasking checks described in NSA's section 702 targeting procedures were not functioning properly, NSA will follow its internal

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) Privileged Communications. NSA may receive unminimized communications, acquired pursuant to section 702 of FISA, to which an attorney is a party. These provisions address the retention, dissemination, and use of information in such communications and apply when NSA personnel handling a communication acquired pursuant to section 702 of FISA determine (based on the information in that communication or other information of which the NSA personnel are aware) that the communication is between an attorney (or any person who, based on the information in the communication, appears clearly to be communicating on behalf of an attorney, such as a paralegal or administrative assistant) and a client.

- (a) (U) After discovering such a communication, if NSA personnel handling a communication determine that the communication does not contain foreign intelligence information or evidence of a crime, the communication must be destroyed irrespective of whether the communication contains information protected by the attorney-client privilege.
- (b) (U) If NSA personnel handling such a communication determine that the communication appears to contain foreign intelligence information or evidence of a crime, the personnel handling the communication must bring the communication to the attention of NSA's Office of General Counsel for action as set forth below.

(c) ~~(S//NF)~~ Privileged Communications Pertaining to a Criminal Charge in the United States.

[REDACTED]

If the communication contains privileged information pertaining to a criminal charge in the United States, the communication shall be segregated.

(d)

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(e)

[Redacted]

(f) ~~(S//NF)~~ Privileged information [Redacted]

[Redacted] shall not be disseminated without the approval of the Office of General Counsel. [Redacted] privileged information from the communication shall not be disseminated outside of the Intelligence Community or the Department of Defense without the approval of the Assistant Attorney General for National Security or his or her designee.

(g) ~~(S//NF)~~ Except as permitted in subparagraph (h) below, dissemination of attorney-client privileged information of the type described in subparagraphs (c) and (e) above outside NSA shall be [Redacted]

[Redacted] accompanied by appropriate handling controls, and shall include language advising recipients (1) that the report contains information obtained from communications that may be subject to the attorney-client privilege, (2) that use of the information is provided for intelligence purposes only and may not be used in any trial, hearing, or other proceeding absent express approval by the Attorney General, and (3) that further dissemination is prohibited absent the express approval of the Assistant Attorney General for National Security [Redacted]

(h)

[Redacted]

(i)

[Redacted]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[REDACTED] NSA shall keep a record of all disseminations outside NSA of attorney-client privileged information of the type described in subparagraphs (c) and (e) above.

(U) Section 5 - Domestic Communications

(U) A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

- (1) (U) such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;
- (2) (U) such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;
- (3) (U) such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.
  - a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

- b. (U) In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Director, Operations Directorate, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

- (4) (U) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

(U) Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) for purposes of collection avoidance. NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

- (1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.
- a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.
- b. (U) In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

- (2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or
- (3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

(U) Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

- (1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;
- (2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;
- (3) (U) the communication or information indicates that the United States person may be:
  - a. an agent of a foreign power;
  - b. a foreign power as defined in section 101(a) of the Act;

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

- c. residing outside the United States and holding an official position in the government or military forces of a foreign power;
  - d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
  - e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;
- (4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;
  - (5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;
  - (6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;
  - (7) (U) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or
  - (8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.
- (c) (U) Provision of Unminimized Communications to CIA, FBI, and NCTC
- (1) (U) NSA may provide to CIA unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.
  - (2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

- (3) (U) NSA may provide to NCTC unminimized communications acquired pursuant to section 702 of the Act [REDACTED]

NCTC will identify to NSA targets for which NSA may provide unminimized communications to the NCTC. NCTC will handle any such unminimized communications received from NSA in accordance with NCTC minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(U) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these

~~TOP SECRET//SI//NOFORN~~

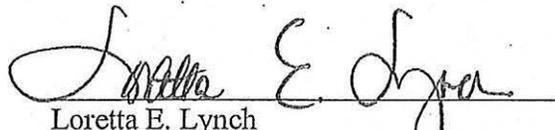
~~TOP SECRET//SI//NOFORN~~

minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

- (1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.
- (2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.
- (3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.
- (4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.
- (5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

SEP 21 2016

Date

  
Loretta E. Lynch  
Attorney General of the United States~~TOP SECRET//SI//NOFORN~~